AMENDMENTS TO THE SPECIFICATION:

Please amend the heading beginning at page 1, line 4 as follows:

TECHNICAL FIELD ~~OF THE INVENTION~~

Please amend the paragraph beginning at page 1, line 6, as follows:

The ~~present invention~~ technical field generally relates to management, implementation and utilization of device-specific security data for various purposes, and more particularly to secure and efficient procedures for providing devices with such device-specific security data.

Please amend the heading beginning at page 11, line 10, as follows:

BACKGROUND ~~OF THE INVENTION~~

Please amend the heading beginning at page 5, line 1, as follows:

SUMMARY ~~OF THE INVENTION~~

Please amend the paragraph beginning at page 5, line 6, as follows:

It is an object ~~of the invention~~ to implement and utilize device-specific security data in devices such as mobile telephones, personal computers, cameras, audio devices, servers, base stations and firewalls.

Please amend the paragraph beginning at page 5, line 10, as follows:

It is an object ~~of the invention~~ to provide a method for securely and cost efficiently manufacturing a device with security data capabilities, as well as a method for management of

security data. In particular, it is desirable to provide the device with tamper-resistantly protected and device-specific security data. It is also important to ensure that security data is protected from unauthorized parties during the entire manufacturing process of the device, without the need for extensive security management.

Please amend the paragraph beginning at page 5, line 18, as follows:

Another object ~~of the invention~~ is to provide an improved method for maintaining data security in relation to network communication between a network device and an external communication partner.

Please amend the paragraph beginning at page 5, line 22, as follows:

Still another object ~~of the invention~~ is to provide an improved method for marking digital content produced by a content-producing device.

Please amend the paragraph beginning at page 5, line 25, as follows:

~~A basic idea according to the invention is to provide a~~ A tamper-resistant electronic circuit ~~that~~ is configured for implementation in a device and that securely implements and utilizes device-specific security data during operation in the device. The tamper-resistant electronic circuit is basically provided with a tamper-resistantly stored secret not accessible over an external circuit interface. The electronic circuit is also provided with functionality for performing cryptographic processing at least partly in response to or based on the stored secret to generate an instance of device-specific security data that is internally confined within said electronic circuit during usage of the device. The electronic circuit is further configured for performing one or more security-

related operations or algorithms in response to the internally confined device-specific security data.

Please amend the paragraph beginning at page 6, line 23, as follows:

The tamper-resistant electronic circuit ~~according to the invention~~ is generally applicable in a wide variety of devices, producing internally confined device-specific security data that can be used for various security-related purposes.

Please amend the paragraph beginning at page 9, line 22, as follows:

In another embodiment ~~of the invention~~, which relates to asymmetric cryptography, suitable additional input such as a prime, a generator of a mathematical group, a nonce and/or a PIN code may be applied to the circuit during configuration of the device, for example during a configuration phase in manufacturing or during user configuration, for generating an asymmetric key pair and for outputting the public key over an external circuit interface. During usage of the device, the corresponding private key is internally generated or re-generated provided that at least part of the same additional input is applied over an external circuit interface.

Please amend the paragraph beginning at page 11, line 4, as follows:

The ~~invention~~ technology also relates to additional security management associated with the device-specific security data, e.g. certification and trust delegation, in order to enable trusted third parties to communicate securely with the network device and/or user.

Please amend the paragraph beginning at page 11, line 8, as follows:

The ~~invention~~ technology offers the following advantages:

Please amend the paragraph beginning at page 12, line 11, as follows:

Other advantages ~~offered by the present invention~~ will be appreciated upon reading of the below description of ~~the~~ example embodiments ~~of the invention~~.

Please delete the paragraph beginning at page 12, line 16, which starts with:

The invention, together...

Please amend the paragraph beginning at page 12, line 20, as follows:

FIG. 1 is a schematic block diagram of a general device provided with a tamper-resistant electronic circuit according to ~~a basic, preferred~~ an example embodiment ~~of the invention~~;

Please amend the paragraph beginning at page 13, line 1, as follows:

FIG. 4 is a schematic flow diagram of a method for manufacturing a device with security data capabilities, including management of device-specific security data, according to ~~a preferred~~ an example embodiment ~~of the invention~~;

Please amend the paragraph beginning at page 13, line 5, as follows:

FIG. 5 is a schematic flow diagram illustrating configuration and usage of trigger data according to an exemplary embodiment ~~of the invention~~;

Please amend the paragraph beginning at page 13, line 8, as follows:

FIG. 6 is a schematic block diagram of a tamper-resistant electronic circuit provided with functionality for encrypting configurational security data into trigger data according to ~~a preferred~~ an example embodiment ~~of the invention~~;

Please amend the paragraph beginning at page 13, line 15, as follows:

FIG. 8 is a schematic block diagram of a tamper-resistant electronic circuit provided with device access code functionality for allowing external access to generated security data during configuration, according to another ~~preferred~~ an example embodiment ~~of the invention~~;

Please amend the paragraph beginning at page 13, line 20, as follows:

FIG. 9 is a schematic block diagram of a tamper-resistant electronic circuit responsive to trigger data for selectively generating an asymmetric key pair/private key according to yet another ~~preferred~~ an example embodiment ~~of the invention~~;

Please amend the heading beginning at page 14, line 19, as follows:

DETAILED DESCRIPTION ~~OF EMBODIMENTS OF THE INVENTION~~

Please amend the paragraph beginning at page 15, line 24, as follows:

The tamper-resistant electronic circuit ~~according to the invention~~ is generally applicable in a wide variety of devices, producing internally confined device-specific security data that can be used for various security-related purposes. Examples of devices suitable for implementing an electronic circuit according to the invention include mobile telephones, personal computers, cameras, audio devices, network servers, security gateways, firewalls, base stations and so forth.

Please amend the paragraph beginning at page 17, line 7, as follows:

Content-marking ~~as suggested by the invention,~~ may be particularly useful in a combination of a network device and a content-producing device, such as a mobile phone with an integrated camera, but is also applicable in stand-alone cameras or similar imaging, video or audio devices.

Please amend the paragraph beginning at page 17, line 13, as follows:

~~In the~~ The following~~[[,]] the invention will~~ is mainly ~~be~~ described with a particular ~~exemplary~~ example scenario in mind, namely manufacturing of devices (also sometimes called entities), including management of initial secrets and/or device-specific security data, and subsequent usage of such security data within the devices. It should though be understood that ~~invention~~ this scenario is not ~~limited thereto~~ limiting~~[[,]]~~. ~~and that the manufacturing scenario merely serves as a basis for a better understanding of the basic concepts and principles of the invention.~~

Please amend the paragraph beginning at page 17, line 21, as follows:

FIG. 4 is a schematic flow diagram of a method for manufacturing a device with security data capabilities, including management of device-specific security data, according to ~~a preferred~~ example embodiment ~~of the invention~~.

Please amend the paragraph beginning at page 20, line 12, as follows:

Accordingly, the parties authorized with device-specific security data may be different for different instances of the described problem. It is assumed throughout the following examples

that the device manufacturer is trusted with the device-specific security data, though the ~~invention~~ technology is ~~actually~~ not limited to that assumption. As indicated above, the chip manufacturer does not need to be trusted with the security data, though some sort of trust relation is normally assumed, e.g. that the chip manufacturer implements what is agreed upon and introduces no secret "back-doors" and so forth. It is also common that the device owner or user is considered a trusted party, since it usually is in his/her interest to ensure that message transfer is secure. However, this is not necessarily t rue and will not be assumed; a particular exemption scenario is that of DRM.

Please amend the paragraph beginning at page 21, line 23, as follows:

With reference once again to FIG. 1, the stored secret C may be the sole input to the cryptographic engine. Alternatively, however, additional input may be applied via the input/output unit 11 of the electronic circuit 10 and used together with the stored secret C in the cryptographic engine 13 to generate the device-specific security data. In ~~a preferred~~ an embodiment ~~of the invention~~, optional trigger data (indicated by the dashed line in FIG. 1) required for generating proper security data is defined during configuration of the device 100, for example in a configuration phase during manufacturing or during user configuration depending on the particular application.

Please amend the paragraph beginning at page 23, line 25, as follows:

FIG. 6 is a schematic block diagram of a tamper-resistant electronic circuit provided with functionality for encrypting configurational security data into trigger data according to ~~a~~ ~~preferred~~ an example embodiment ~~of the invention~~. Preferably, the electronic circuit 10 is

configured for generating trigger data as a cryptographic representation of some configurational device-specific security data, based on the stored secret. The cryptographic representation is then output over an external circuit interface during the configuration phase. During usage of the device, the device-specific security data is internally re-generated provided that said additional input corresponds to the cryptographic representation. This allows the device manufacturer or other trusted party in control of the devices, such as a network operator, to freely select device-specific security data for manufactured devices during device configuration. This may be advantageous in certain applications where the security data is requited to have a particular format. For example, in asymmetric cryptography such as RSA or elliptic curves, the keys are not just random strings but rather have to be chosen with caution.

Please amend the paragraph beginning at page 31, line 12, as follows:

FIG. 9 is a schematic block diagram of a tamper-resistant electronic circuit responsive to trigger data for selectively generating a private key/an asymmetric key pair according to yet another ~~preferred~~ embodiment ~~of the invention~~. In FIG. 9, suitable additional input such as a prime, a generator of a mathematical group, a nonce and/or a PIN code may be applied to the circuit during configuration of the device, either during a configuration phase in manufacturing or during user configuration, for generating an asymmetric key pair (A, P.sub.A) and for outputting the public key P.sub.A over an external circuit interface. During usage of the device, the corresponding private key A is internally re-generated provided that at least part of the same additional input is applied as trigger data over an external circuit interface. The internally generated private key A may then be used for PKI (Public Key Infrastructure) operations such as encryption/decryption and authentication.